

CLAIMS

What is claimed is:

- 1 1. A machine-implemented method for managing access to data, the method comprising
2 the steps of:
3 detecting that a database command is issued;
4 wherein said database command requires access to at least one column in a table;
5 rewriting said database command by creating a modified database command, based
6 on the database command;
7 wherein the modified database command specifies whether to mask a value of at least
8 one column by returning a mask of the value instead of the value; and
9 executing said modified database command.
- 1 2. The method of claim 1,
2 wherein said database command requests at least two values located in at least two
3 columns;
4 wherein each of the two values are located in a different one of the at least two
5 columns; and
6 wherein the step of executing the modified database command includes at least
7 returning at least one of the at least two values, and
8 returning a masked value instead of at least a second of the at least two values.
- 1 3. The method of claim 1, wherein the modified database command
2 includes at least
3 a condition expression returned by a policy function.

- 1 4. The method of claim 1, wherein the masked value is returned for rows
2 that
3 are retrieved for the database command issued,
4 do not satisfy the condition, and
5 to which access privileges are granted.
- 1 5. The method of claim 1, further comprising:
2 storing metadata that associates a list of one or more columns with a policy used for
3 controlling access to the one or more columns;
4 wherein the step of rewriting is performed if a match is found between the at least one
5 column to which the database command requires access and the list of one or
6 more columns.
- 1 6. The method of claim 1, further comprising:
2 storing metadata that associates a list of one or more columns with a policy used for
3 controlling access to the one or more columns;
4 wherein the step of creating is not performed if a match is not found between the list
5 of one or more columns and the at least one column to which the database
6 command requires access.
- 1 7. The method of claim 1, further comprising:
2 creating a policy function that returns a condition expression;

3 wherein the step of creating the modified database command includes incorporating
4 the condition expression and the database command into the modified
5 database command.

1 8. The method of claim 7, further comprising:
2 creating a policy referencing the policy function and specifying trigger columns that
3 trigger implementing the policy.

1 9. The method of claim 1, further comprising registering a policy function with a
2 database server, wherein the policy function returns a condition expression and the
3 modified database command is based on the condition expression.

1 10. A machine-implemented method for managing access to data, the method comprising
2 the steps of:
3 detecting that a database command is issued;
4 detecting that said database command requires access to at least one column in a
5 table;
6 in response to detecting that the database command requires access to the at least one
7 column, creating a modified database command by selectively adding zero or
8 more predicates that are satisfied by rows in said table to which said user is
9 permitted access.

1 11. A machine-readable medium carrying one or more sequences of instructions, which
2 when executed by one or more processors, causes the one or more processors to
3 perform a method comprising the steps of:

4 detecting that a database command is issued;
5 wherein said database command requires access to at least one column in a table;
6 rewriting said database command by creating a modified database command, based
7 on the database command;
8 wherein the modified database command specifies whether to mask a value of at least
9 one column by returning a mask of the value instead of the value; and
10 executing said modified database command.

1 12. The machine readable medium of claim 1,
2 wherein said database command requests at least two values located in at least two
3 columns;
4 wherein each of the two values are located in a different one of the at least two
5 columns; and
6 wherein the step of executing the modified database command includes at least
7 returning at least one of the at least two values, and
8 returning a masked value instead of at least a second of the at least two values.

1 13. The machine-readable medium of claim 1, wherein the modified
2 database command includes at least
3 a condition expression returned by a policy function.

1 14. The machine-readable medium of claim 1, wherein the masked value is
2 returned for rows that
3 are retrieved for the database command issued,

4 do not satisfy the condition, and
5 to which access privileges are granted.

1 15. The machine-readable medium of claim 1, wherein the method further comprises:
2 storing metadata that associates a list of one or more columns with a policy used for
3 controlling access to the one or more columns;
4 wherein the step of rewriting is performed if a match is found between the at least one
5 column to which the database command requires access and the list of one or
6 more columns.

1 16. The machine-readable medium of claim 1, wherein the method further comprises:
2 storing metadata that associates a list of one or more columns with a policy used for
3 controlling access to the one or more columns;
4 wherein the step of creating is not performed if a match is not found between the list
5 of one or more columns and the at least one column to which the database
6 command requires access.

1 17. The machine-readable medium of claim 1, wherein the method further comprises:
2 creating a policy function that returns a condition expression;
3 wherein the step of creating the modified database command includes incorporating
4 the condition expression and the database command into the modified
5 database command.

1 18. The machine-readable medium of claim 7, wherein the method further comprises:

2 creating a policy referencing the policy function and specifying trigger columns that
3 trigger implementing the policy.

1 19. The machine-readable medium of claim 1, wherein the method further comprises
2 registering a policy function with a database server, wherein the policy function
3 returns a condition expression and the modified database command is based on the
4 condition expression.

1 20. A machine-readable medium carrying one or more sequences of instructions, which
2 when executed by one or more processors, causes the one or more processors to
3 perform a method comprising the steps of:
4 detecting that a database command is issued;
5 detecting that said database command requires access to at least one column in a
6 table;
7 in response to detecting that the database command requires access to the at least one
8 column, creating a modified database command by selectively adding zero or
9 more predicates that are satisfied by rows in said table to which said user is
10 permitted access.